Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended) A method for securing an imaging job, the method comprising:

performing an access control function relating to a document;

performing an auditing function relating to the document, including extracting reduced

content information from the document and storing the reduced content

information in secured storage as at least part of an audit trail generated by the

auditing function;

generating an imaging job from the document;

encrypting content of the imaging job and not encrypting non-content such that a

downstream non-content dependent process will still properly process the imaging

job;

decrypting the encrypted content by a recipient;

encoding into imaging output non-destructible information; and

erasing residual data containing any content of ~~that relates to~~ the imaging job both on a

client device and an imaging device, the content of the imaging job comprising

instructions configured to produce visible information on the imaging output.

2.   (Canceled)

3.   (Original) The method of claim 1, further comprising transmitting the imaging job from
a client to the recipient, and wherein the transmitting is performed in between the encrypting and
the decrypting.

4.   (Original) The method of claim 1, wherein the actions are performed in the order as
listed.

5.   (Original) The method of claim 1, wherein the access control function determines if a user has authorization to perform a certain operation by using access control information.

6.   (Original) The method of claim 5, wherein the access control information comprises data that is selected from the group consisting of a login identification, a department code, client device identification, recipient device identification, imaging operation, meta-data, a serial number, a network address, a digital signature and biometric data.

7.   (Original) The method of claim 1, wherein the access control function determines authorized content and causes the authorized content to be processed to create the imaging job.

8.   (Canceled)

9.   (Original) The method of claim 1, wherein the non-destructible information encoded into the imaging output comprises tracking information.

10.   (Original) The method of claim 9, wherein the tracking information comprises client tracking information and imaging device tracking information.

11.   (Currently Amended) A system ~~configured to implement a method~~ for securing an

imaging job, the system comprising:

      a client device having a processor and memory in communication with the processor;

      client executable instructions stored in the memory, wherein the client executable

            instructions are executable to:

            perform an access control function relating to a document;

            perform an auditing function relating to the document, including extracting

                reduced content information from the document and storing the reduced

                content information in secured storage as at least part of an audit trail

                generated by the auditing function;

            generate an imaging job from the document;

            encrypt content of the imaging job and not encrypting non-content such that a

                downstream non-content dependent process will still properly process the

                imaging job; and

            erase first residual data <u>containing any content of</u> ~~that relates to~~ the imaging job

                <u>on the client device, the content of the imaging job comprising instructions</u>

                <u>configured to produce visible information on imaging output;</u>

      a recipient <u>imaging</u> device; and

      recipient executable instructions executable on the recipient device, wherein the recipient

            executable instructions are executable to:

            decrypt the encrypted content;

            encode into <u>the</u> imaging output non-destructible information; and

            erasing second residual data <u>containing any content of</u> ~~that relates to~~ the imaging

                job <u>on the recipient imaging device.</u>

12.   (Canceled)

13.   (Original) The system of claim 11, wherein the method of the client executable

instructions further comprises transmitting the imaging job from the client device to the recipient

device, and wherein the transmitting is performed after the client device encrypts the content.

14.   (Original) The system of claim 11, wherein the access control function determines if a user has authorization to perform a certain operation by using access control information.

15.   (Original) The system of claim 14, wherein the access control information comprises data that is selected from the group consisting of a login identification, a department code, client device identification, recipient device identification, imaging operation, meta-data, a serial number, a network address, a digital signature and biometric data.

16.   (Original) The system of claim 11, wherein the access control function determines authorized content and causes the authorized content to be processed to create the imaging job.

17.   (Canceled)

18.   (Original) The system of claim 11, wherein the non-destructible information encoded into the imaging output comprises tracking information.

19.   (Original) The system of claim 18, wherein the tracking information comprises client tracking information, imaging device tracking information, user tracking information and content tracking information.

20.   (Currently Amended) A computer-readable medium storing program data, wherein the program data comprises executable instructions ~~implementing a method~~ for securing an imaging job, the method comprising:

>   performing an access control function relating to a document;
>
>   performing an auditing function relating to the document, including extracting reduced content information from the document and storing the reduced content information in secured storage as at least part of an audit trail generated by the auditing function;
>
>   generating an imaging job from the document;
>
>   encrypting content of the imaging job and not encrypting non-content such that a downstream non-content dependent process will still properly process the imaging job;
>
>   decrypting the encrypted content by a recipient;
>
>   encoding into imaging output non-destructible information; and
>
>   erasing residual data <u>containing any content of</u> ~~that relates to~~ the imaging job <u>both on a client device and an imaging device, the content of the imaging job comprising instructions configured to produce visible information on the imaging output.</u>

21.   (Canceled)

22.   (Previously Presented) The computer-readable medium of claim 20, wherein the method further comprises transmitting the imaging job from a client to the recipient, and wherein the transmitting is performed in between the encrypting and the decrypting.

23.   (Original) The computer-readable medium of claim 22, wherein the actions are performed in the order as listed.

24.   (Original) The computer-readable medium of claim 23 wherein the access control function determines if a user has authorization to perform a certain operation by using access control information.

25.   (Original) The computer-readable medium of claim 24, wherein the access control information comprises data that is selected from the group consisting of a login identification, a department code, client device identification, recipient device identification, imaging operation, meta-data, a serial number, a network address, a digital signature and biometric data.

26.   (Original) The computer-readable medium of claim 24, wherein the access control function further determines authorized content and causes the authorized content to be processed to create the imaging job.

27.   (Canceled)

28.   (Previously Presented) The computer-readable medium of claim 26, wherein the non-destructible information encoded into the imaging output comprises tracking information.